Security Work Group
http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

Monday March 31, 2003
10:00 A.M. to Noon
NSOB 6Y – Lincoln, NE

Minutes

A. Participants

Allan	Albers	HHSS
Randy	Cecrle	Workers Compensation
Steve	Cherep	HHSS
Cathy	Danahy	Secretary of State / Records Management
Jerry	Hielen	IMServices
Keith	Larson	HHSS
Scott	McFall	State Patrol
Leona	Roach	University of Nebraska
Linda	Salac	HHSS
Steve	Schafer	Nebraska CIO
Eric	Wieczorek	Military
Ron	Woerner	Department of Roads

A. Discuss Secure Communications

Randy Cecrle introduced the topic of secure e-mail and other type of electronic communications. HIPAA, the Bureau of Labor Statistics and other federal entities are requiring "certified" secure communications for certain types of information. This presents both technical and procedural issues.

The technical issues include:

- Setting up cross-certification among different NOTES domains;
- How to set up cross-certification between heterogeneous environments (e.g., NOTES and Exchange);
- Configuring port encryption (?) on servers.

Procedural issues include:

- Prohibiting using e-mail for confidential information, unless the communication links are secure;
- Establishing a process for certifying "trusted relationships" between agency environments that addresses technical and procedural issues;
- Training employees to know when it is safe to use e-mail for sending confidential information;

Several agencies may be interested in cross certifying their e-mail systems. Keith Larson suggested adopting a policy that state government should strive toward a seamless secure system. It should be easy for the user to determine what is secure and what is not. Users need education to know when and how to send secure e-mail. And the policy should address the compliance issue for maintaining certified environments.

Secure communication should cover FTP, HTTP, and other communications, in addition to e-mail. Randy Cecrle, Keith Larson, and Jerry Hielen will work on developing a first draft.

B. Discuss Draft NITC Wireless Security Policy

Comments and suggestions included:

- Replace "shall" with "should" throughout the document, since this is intended to be a guideline;
- Clarify the applicability for higher education, especially regarding notification when implementing wireless technology. The guidelines should encourage notification of the central entity managing a network. For state government agencies, that is DAS. For K-12 and higher education, it would be the manager of their respective networks;
- Delete all of the detailed material in the Executive Summary, since most of this information is also provided in Section D, Guidelines;
- Assign the task of monitoring for rogue wireless connections to whomever has network management responsibilities, by periodically scanning for unregistered nodes on the network;

C. Discuss Remote Access Policy

Comments and suggestions included:

- Eliminate references to the "federal" government;
- Clarify the applicability to K-12 and higher education, with the same type of changes as those discussed regarding the wireless security policy.

D. Update on Directory Services Project

Jerry Hielen described the process for working on details for setting up the directory services. IMServices and the Office of the CIO are jointly sponsoring workgroup sessions with representation by participating agencies.

E. State Network Security Issues

1. Update on Security Assessment. Steve Schafer explained the status of the external intrusion security assessment. Omni Tech has completed Phase I, discovery, and will report their findings at a conference call on Wednesday morning (April 2).
2. Discussion of network security standards. Steve Schafer will check with Steve Henderson on the status of their proposed standards for the state's network. Discussion included a suggestion of some means for sharing information about testing security patches. This would save agencies time and provide greater confidence about the potential impact of installing security patches. There is also an issue about the responsibility of third party applications to stay current with security patches. Agencies should address this issue in their contracts.

F. Security Awareness

Jerry Hielen reported on efforts to explore a new pricing model, if IMServices hosted the application.

G. Update on Disaster Planning

Steve Schafer reported on potential activities relating to business continuity planning. He will report back at the next meeting.

B. Next Meeting Dates

The next meeting is Tuesday May 6 at 10:00. The location is the NSOB LLF.

Security Newsletters And Alerts

SANS

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

SANS NewsBites - weekly

NewsBites saves you from having to read every trade publication and newspaper to find the key security stories. It keeps up with everything going on in the computer security world. A dozen or two articles, each just one, two, or three sentences in length, elaborate a URL that points to the source of the detailed information.
Review samples.

Critical Vulnerability Analysis Newletter - weekly

The new Critical Vulnerability Analysis report is delivered every Monday morning. It focuses on the three to eight vulnerabilities that matter, tells what damage they do and provides data on the actions 15 giant organizations took to protect themselves.
Review samples.

Security Alert Consensus (SAC) - weekly

One definitive weekly summary of new alerts and countermeasures each week with announcements from: SANS, CERT, the Global Incident Analysis Center, the National Infrastructure Protection Center, the Department of Defense, Security Portal, Ntbugtraq, Sun, Microsoft and several other vendors. When you subscribe, by selecting only the operating systems you support, you will receive a version of Security Alert Consensus tailored and customized to your needs: just pick the operating systems you want included in your customized weekly digest.
Review samples.

For a free subscription, (and for free posters) visit http://www.sans.org/sansnews/

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings - DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications - DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other Publications DHS/IAIP Daily Reports Archive - Access past DHS/IAIP Daily Open Source Infrastructure Reports